UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/721,504	11/26/2003	Franck Le	60282.00102	6168

32294 7590 12/05/2008
SQUIRE, SANDERS & DEMPSEY L.L.P.
8000 TOWERS CRESCENT DRIVE
14TH FLOOR
VIENNA, VA 22182-6212

EXAMINER	
HENNING, MATTHEW T	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
12/05/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/721,504	LE ET AL.	
	Examiner	Art Unit	
	MATTHEW T. HENNING	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 October 2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-15,18,42-64 and 66-68* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-15,18,42-64 and 66-68* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 November 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

This action is in response to the communication filed on 10/15/2008.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/15/2008 has been entered.

Response to Arguments

Applicant's arguments filed 10/15/2008 have been fully considered but they are not persuasive.

Regarding applicants' argument that there would be no burden on the examiner to consider the improperly cited references from the IDS submitted 11/26/2003 is not found persuasive. The issue is not one of burden, but rather lies in the fact that the citations were not proper, as required by the 37 CFR 1.98 (b)(5). For example, if the citation does not include the number pages of the submitted reference, how can the examiner accurately determine that the entirety of the document has been considered. As such, the examiner will not consider these references until they are submitted in an IDS with proper citations.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., there are only two nodes in the communication system) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). In this case, the applicants have argued that in the teachings of Gupta, there is a third node. However, there is nothing in the claim language that forbids this from being the case, as the claims are recited using the language "comprising". As such, the examiner does not find the argument persuasive.

Regarding the applicants' argument that Gupta does not disclose that "no pre-established security association is needed to verify the packet", the examiner does not find the argument persuasive. The applicants argue that the validity information in Gupta is pre-established. This is not forbidden by the claim language. The applicants argue that in Gupta, the sender establishes a public and private key pair with a DNS server, and therefore pre-established a security association. The examiner disagrees. The instant specification paragraph 0004 indicates that a security association is part of IPSec, which Gupta does not disclose the use of IPSec, and that the security association is "a set of policy and key(s) used to protect information". The instant specification paragraph 0054 further states, with regards to the lack of pre-established security association, that "the nodes do not need to have any pre-established [security association], or have to exchange key values beforehand". Gupta disclosed with regards to Fig. 7, that upon receipt of a signed packet, the router will check to see if it has the proper validation key, and if not it will get the key from a DNS server, or a certification server. In this case, it is clear that the key needed to validate the packet was not exchanged between the sender and the router, and certainly not before receipt of the packet. As such, a security association was not pre-established. Therefore, the examiner does not find the argument persuasive.

The examiner notes that the applicants appear confused by the Gupta reference, wherein they have argued that the owner is the receiver of the message. Note that in Gupta, the router is the second node of the network, which performs the verification. This can be seen in Fig. 7 and the corresponding text.

Regarding the applicants' argument that the header of the packet of Gupta does not contain "all" information necessary to perform the validity check, the examiner still does not find this argument persuasive. The applicants' use the language "all necessary information required for performing a validity check" throughout the specification. In order to remain consistent with the specification, the examiner has looked to the instant specification in order to interpret the usage of this language, for the purposes of searching and applying prior art. The specification provides evidence that this limitation means "all necessary information required for performing a validity check **without the checking entity needing to further communicate with the sending network node**", as the specification clearly shows that the checking node does not require further communication with the sending node in order to perform the validity checking, but that the checking entity may need to receive additional information from somewhere (i.e. a certificate authority) in order to perform the validity checking. As such, if Gupta disclosed that the key was retrieved from the DNS server, or that the algorithm to perform the verification was known by the verifier, this would still fall within the scope of the language, in light of the specification. Therefore, the examiner does not find the argument persuasive.

Regarding the applicants' argument with regards to Naudus, that a security association requires pre-establishment, the examiner does not find the argument persuasive. The rejection does not rely upon this teaching of Naudus, but rather relies upon the teaching of Naudus that including timestamps in a packet prevents replay attacks. As such, the examiner does not find the argument persuasive.

Further, rather than claiming what the invention is not, the examiner suggests that the applicants carefully consider the meets and bounds of their invention, and then carefully construct positive claim limitations which accurately define that scope. For example, if the applicants believe that it is important to their invention that the algorithm and key used for verification is provided in the header of the packet, then the applicants should particularly point that out in the claim language.

The examiner has maintained the prior art rejections previously set forth.

All objections and rejections not set forth below have been withdrawn.

Claims 1-2, 4-15, 18, 42-64, and 66-68 have been examined.

Information Disclosure Statement

The information disclosure statement(s) (IDS) submitted on 11/26/2003 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statements. However, the examiner notes, as indicated on the signed copy, that the references listed in the IDS did not properly identify the pertinent pages of each reference, and as such were not considered. See MPEP Section 609.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 66-68 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 66-68 are directed towards software *per se*, which has been held by the courts as non-statutory. Because the software, as claimed, is not embodied in a statutory medium, it is simply software *per se*. If, however, it were claimed as being embodied on a computer readable storage medium, which does not include transmission media, the examiner believes, at this time, that the claims would be statutory. No new matter will be permitted. See MPEP 2106.01(I)

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-2, 5-10, 15, 18, 42-43, 45-49, 54-56, 58-60, and 62-64, and 66-68 are rejected under 35 U.S.C. 102(b) as being anticipated by Gupta et al. (US Patent Number 6,389,532) hereinafter referred to as Gupta.

Regarding claims 1 and 66, Gupta disclosed a method (See Gupta Fig. 1 Element 104, 108 or 112), comprising the steps of: generating validity information for a packet (See Gupta Figs. 5-6 and Col. 6 Paragraphs 2-4), wherein the validity information comprises all necessary information required to perform a validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2); the validity information comprising algorithm information to be used for performing the validity check of the packet and no pre-established security association is needed to verify the packet (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4);

generating a packet header (302), comprising the validity information (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4); and sending the packet including the header from a first network node to a second network node (See Gupta Col. 6 Paragraph 4).

Regarding claim 18, Gupta disclosed an apparatus comprising: validity information generating means for generating validity information for a packet (See Gupta Figs. 5-6 and Col. 6 Paragraphs 2-4); packet header generating means for generating a header for the packet, comprising the validity information (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4); and sending means for sending the packet including the header to a receiving network node (See Gupta Col. 6 Paragraph 4), wherein the validity information comprises all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2) and the validity information comprises algorithm information to be used for performing the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4).

Regarding claim 42, Gupta disclosed an apparatus, comprising: a validity information generator configured to generate validity information for a packet (See Gupta Figs. 5-6 and Col. 6 Paragraphs 2-4); a packet header generator configured to generate a header for the packet, comprising the validity information (See Gupta Fig. 3 and Col. 6 Paragraphs 3-4); and a transmitter configured to send the packet including the header to a receiving network node (See Gupta Col. 6 Paragraph 4), wherein the validity information comprises all necessary information required to perform a validity check of the packet and no pre-established security association is needed to verify the packet, and the validity information comprises algorithm information to be used to perform the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 3 - Col. 7 Paragraph 2).

Regarding claim 55, Gupta disclosed an apparatus, comprising: a receiver configured to receive packets from a sending network node (See Gupta Fig. 1 Element 108, Fig. 7 and Col. 6 Paragraph 5); and a checker configured to perform a validity check of a packet by referring to validity information contained in a header of the packet and no pre-established security association is needed to verify the packet (See Gupta Fig. 7 and Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required to perform the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2), and the validity information comprises algorithm information to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4).

Regarding claim 59, Gupta disclosed an apparatus, comprising: a transmitter configured to forward packets from a sending network node to a receiving network node (See Gupta Fig. 7 and Col. 6 Paragraph 5); and a checker configured to perform a validity check of a packet by referring to validity information contained in a header of the packet (See Gupta Fig. 7 and Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required to perform a validity check of the packet and no pre-established security association is needed to verify the packet (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2), and the validity information comprises algorithm information to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4).

Regarding claims 63 and 67, Gupta disclosed a method comprising: receiving packets (See Gupta Fig 7 and Col. 6 Paragraph 5 - Col. 7 Paragraph 2); and performing a validity check of a packet by referring to validity information contained in a header of the packet (See Gupta Fig. 7 and Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required for performing the validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 3 - Col. 7 Paragraph 2).

Regarding claims 64 and 68, Gupta disclosed a method comprising: forwarding received packets (Gupta Col. 7 Paragraph 2); and performing means for performing a validity check of a packet by referring to validity information contained in a header of the packet (Gupta Col. 7 Paragraph 2), wherein the validity information comprises all necessary information required for performing a validity check of the packet and no pre-established security association is needed to verify the packet, the validity information comprising algorithm information to be used for performing the validity check of the packet (See Gupta Fig 7 and Col. 6 Paragraph 3 - Col. 7 Paragraph 2).

Regarding claims 2, 43, 56 and 60, Gupta disclosed that the generating of the validity information comprises generating security information indicating security services applied to the packet (See Gupta Col. 5 Paragraph 7).

Regarding claim 5, Gupta disclosed that the generating the algorithm information comprises generating of the algorithm information which comprises values to initialize an algorithm to be used to perform the validity check of the packet (See Gupta Col. 6 Paragraphs 3-4, the data, the key index, the signature, or the fingerprint, for example).

Regarding claims 6, 45, 58, and 62, Gupta disclosed that the generating of the validity information comprises generating public key information of a sending node (See Gupta Col. 6 Paragraphs 2-6, for example the public and private key pair, or the key index).

Regarding claims 7, and 46 Gupta disclosed that the generating of the public key information comprises generating reference information related to how a public key can be obtained (See Gupta Col. 6 Paragraphs 3-4 and Col. 7 Paragraph 2).

Regarding claims 8, and 47, Gupta disclosed that the generating of the reference information comprises generating an identity of an entity from which the public key can be obtained (See Gupta Col. 6 Paragraphs 3-4, Col. 7 Paragraph 2, and Col. 3 Line 64 – Col. 4 Line 13, wherein the index is the identity, and the entry in the table is the entity).

Regarding claims 9, and 48, Gupta disclosed that the generating of the reference information comprises generating a public key identifier for the public key (See Gupta Col. 6 Paragraphs 3-4 and Col. 7 Paragraph 2, the key index).

Regarding claim 10, and 49, Gupta disclosed that the generating of the public key information comprises generating the public key (See Gupta Col. 6 Paragraph 2).

Regarding claim 15 and 54, Gupta disclosed signing the packet using a private key corresponding to a public key indicated by the validity information in the packet header in a sending network node (See Gupta Col. 6 Paragraph 4).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

Claims 4, 12-14, 44, 51-53, 57, and 61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta as applied to claims 1, 18, 19, and 20 above, and further in view of Naudus (US Patent Number 6,202,081).

Regarding claims 12-14, and 51-53, Gupta disclosed validation of packets, but failed to disclose that the step of generating the validity information comprises generating an information item for preventing replay attacks.

Naudus teaches that in a packet filtering system, packets should include timestamps in order to prevent replay attacks. Naudus further teaches that "[r]eplay attacks occur when a malicious user gains access to a router or other network device on a computer network that is forwarding data packets. Legitimate data packets are intercepted and then re-sent at a later time to allow the malicious user to appear as a legitimate user. A firewall helps prevent replay attacks by checking a time-stamp in the data packet that prevents the data packets from being re-sent at a later time." (See Naudus Col. 2 Paragraph 4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Naudus in the packet validity checking system of Gupta by including a timestamp in each packet and verifying the timestamp at the validity checker. This would have been obvious because the ordinary person skilled in the art would have been motivated to prevent replay attacks in the network. In this combination, the inclusion of a timestamp in each packet, in itself, is an indication of a procedure to be used for anti replay attacks.

Regarding claims 4, 44, 57, and 61, Gupta did not specifically teach that the step of generating the algorithm information comprises generating the algorithm information which indicates an algorithm to be used for performing the validity check of the packet. However, as taught by Naudus, in Col. 6 Line 60 - Col. 7 Line 7, it is well known to include in the packet header, an identification of which algorithm was used to sign the packet. As such, it would have been obvious to have included this information within the packet. Furthermore, the ordinary person skilled in the art at the time of invention would have recognized that this would allow for the user of a multiplicity of signature algorithms, as well as allowing updating of the signature algorithms in the future, and therefore it would have been obvious to have included an indication of the signature algorithm in the packet.

Claims 11, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta as applied to claims 6 and 23 above, and further in view of Nikander (US Patent Number 7,155,500).

Gupta disclosed including public key information within the packets, but failed to specifically disclose including the public key itself within the packets or that the step of generating the public key information comprises generating public key verification information indicating information in order to verify that the public key actually belongs to the sending node.

Gupta did disclose that the public and private key pairs can be generated and stored in a certification server (See Col. 4 Paragraph 2).

Nikander teaches that by including a public key itself and the certificate of the public key, the receiving host can verify that the public key is truly owned by the sender (See Nikander Col. 10 Line 50 – Col. 12 Line 9).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Nikander in the packet verification system of Gupta by including the public key and public key certificate within each packet and verifying that the sender of each packet owned the public key used to sign the packet. This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that a malicious node was not claiming to be a different node.

Conclusion

Claims 1-2, 4-15, 18, 42-64, and 66-68 have been rejected.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew T Henning/
Examiner, Art Unit 2431